

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"  
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ  
Комп'ютерний практикум

Робота №1

Виконали:  
Сернова А.Р., Колесник А.М.  
студенти групи ФБ-93

Перевірила:  
Селюх П.В.

Київ-2021

**Мета роботи:** Засвоєння понять ентропії на символ джерела та його надлишковості, вивчення та порівняння різних моделей джерела відкритого тексту для наближеного визначення ентропії, набуття практичних навичок щодо оцінки ентропії на символ джерела

**Постановка задачі:** реалізувати програму, що підраховує значення ентропії для літер та біграм (з перетином та без) у текстовому файлі, як з урахуванням пробілів, так і без них.

Під час виконання лаб. роботи виникли деякі труднощі: найбільша це вибір іншої мови програмування (вона була обрана через те, що python – дуже багата на функції з рядками мови), також деякі труднощі з фільтруванням тексту, які ми вирішили за допомогою різних інтернет ресурсів таких як stackoverflow та подібних. Дещо виникали складності під час початку роботи з біграмами, а саме продумування варіантів та алгоритмів їх підрахунку, які були вирішені розбиттям тексту на біграми і використання функції count.

Нижче наведені таблиці для літер російського алфавіту без «ё» і «ъ» без урахування пробілів (таб. 1), та з пробілами (таб. 2)

о	0.1101
е	0.0841
а	0.0790
т	0.0661
и	0.0657
н	0.0629
с	0.0552
л	0.0454
р	0.0430
в	0.0410
к	0.0388
м	0.0319
у	0.0292
п	0.0288
д	0.0287
я	0.0240
ы	0.0196
ь	0.0193
г	0.0176
ч	0.0173
з	0.0168
б	0.0163
й	0.0104
ж	0.0100
х	0.0094
ш	0.0091
ю	0.0069
щ	0.0041
э	0.0034

—	0.1644
о	0.0920
е	0.0703
а	0.0660
т	0.0552
и	0.0549
н	0.0526
с	0.0462
л	0.0378
р	0.0359
в	0.0343
к	0.0324
м	0.0267
у	0.0244
п	0.02404
д	0.02402
я	0.0200
ы	0.0163
ь	0.0162
г	0.0147
ч	0.0145
з	0.0141
б	0.0136
й	0.0087
ж	0.0084
х	0.0079
ш	0.0076
ю	0.0058
щ	0.0035



Для біграм з урахуванням пробілів наведено фрагменти з отриманого файлу after.txt: з перетинами (*таб. 6*) та без (*таб. 5*)

110 Bigram for no cross, with spaces  
111 aa is 2.264729945108608e-05 a6 is 0.0009993120882791733 am is 0.0026200094552475206 ar is 0.0005760906797870021 ad is 0.0017848902679887215 ae is 0.0033192448257998034 ak is 0.0013404370362611574 aa is 0.0032130856096228375 am is 0.0001910865891185388 ай is 0.0006029843478851668 ак is 0.005315038089926764 an is 0.007523149786407657 am is 0.003347553950113661 am is 0.0027459850584441873 ao is 6.794189835325824e-05 an is 0.0008110564115920202 ap is 0.0018896340479499947 ac is 0.0036419688429777802 at is 0.004499735309687666 ay is 0.00014296107778498086 aф is 0.00010757467239265888 ax is 0.001143688622279847 au is 0.00011040558482404464 av is 0.0013390215800454645 aw is 0.0008818292223766643 aш is 0.0003269703858250553 aw is 0.0 аь is 0.0 аа is 1.41545621569288e-06 aw is 0.000207116913852504 ay is 0.002195372590539657 a is 0.013357660307493708  
112 6a is 0.0012951424373589852 66 is 1.4154562156928799e-05 6b is 3.114003674524336e-05 6r is 1.22318432353932e-05 6d is 1.132364972554304e-05 6e is 0.001791967569067186 6ж is 9.90819350985016e-06 6a is 9.90819350985016e-06 6b is 0.0008563510104941924 6й is 0.0 6к is 0.00012880651562805208 6н is 0.0006850808083953539 6м is 4.529459890217216e-05 6н is 0.00028450669935426885 6o is 0.0018287694306752009 6п is 0.0 6р is 0.001074331267710896 6с is 0.0001981638701970032 6т is 1.4154562156928799e-05 6у is 0.0011252876914758397 6ф is 0.0 6х is 3.255549296093624e-05 6ц is 7.0772810784643995e-06 6ч is 7.0772810784643995e-06 6ш is 4.24636864707864e-06 6щ is 0.00028592215556996173 6ы is 0.002804018763287595 6ь is 0.00023496573180501807 6а is 0.0 6б is 4.24636864707864e-06 6б is 0.0006043998041008597 6 is 0.00020099478262838896  
113 va is 0.005789215922183879 v6 is 8.49273729415728e-06 vв is 4.24636864707864e-05 vr is 1.273910594123592e-05 vd is 0.0002406275566677896 ve is 0.003971770141234221 vx is 9.90819350985016e-06 va is 0.00043737597064909993 vi is 0.002444492884501604 vй is 0.0 vk is 0.00021373388856962488 vl is 0.0006935735456895112 vm is 0.00011040558482404464 vn is 0.0009257083650631435 vo is 0.0057651531665171 vp is 0.000179762939392959777 wr is 0.0006850808083953539 ws is 0.0025209275201490194 vt is 0.0003085694550210478 vy is 0.0005576097489829948 wf is 1.41545621569288e-06 wx is 4.104823025509352e-05 wц is 2.972458052955848e-05 wч is 6.794189835325824e-05 wш is 0.0007374526883759904 wщ is 0.0 wy is 0.00240344465424651 wь is 0.00010191284752988736 wа is 0.0 wб is 4.24636864707864e-06 wб is 0.0003382940355505983 w is 0.005419781049880038  
114 ra is 0.0011564277282210828 r6 is 0.0 rb is 1.4154562156928799e-05 rr is 1.41545621569288e-06 rd is 0.001166335921730933 re is 0.00013871470913790225 rg is 0.0 rз is 4.24636864707864e-06 ri is 0.0008648437477883497 rй is 0.0 rk is 8.775828537295856e-05 rl is 0.0014310262340655017 rm is 8.49273729415728e-06 rn is 0.0002618593999031828 ro is 0.00075330579979175075 ri is 2.83091243138576e-06 rp is 0.0008563510104941924 rs is 1.698547458831456e-05 rr is 4.387914268647928e-05 ry is 0.0006143079976107099 rф is 0.0 rг is 0.0 rц is 0.0 rч is 3.963277403940064e-05 rw is 2.83091243138576e-06 rх is 0.0 rу is 0.0 rь is 0.0 rа is 0.0 rб is 0.0 rв is 0.0 rг is 0.0 rд is 0.0 rе is 0.0006100616289636312  
115 da is 0.00392647542323049 d6 is 7.218826700033687e-05 dа is 0.0009625102266711584 dr is 1.698547458831456e-05 dd is 2.689366809816472e-05 de is 2.689366809816472e-05 de is 0.0006100616289636312 du is 4.81251133355792e-05 dm is 9.342011023573007e-05 ds is 1.4154562156928799e-05 di is 0.00223217445521476717 dй is 0.0 dk is 0.0002250575382951679 dл is 0.0006100616289636312 du is 4.81251133355792e-05 dn is 0.0015357699940267747 do is 0.003956200122861599 dp is 0.00012314469076528056 dр is 0.0011083022168875251 ds is 0.000257613833125610417 dt is 0.00022364208207947502 e is 0.017674801765356993  
116 ea is 5.378733619632944e-05 e6 is 0.0013376061238297716 ev is 0.001331944298967 er is 0.0033801094430745975 ed is 0.002535082082305948 ee is 0.001320620649241457 ej is 0.000728959951081831 ez is 0.0012441860135940415 ei is 7.643463564741552e-05 ej is 0.001585109615760255 ek is 0.0011394422536327683 el is 0.00455322645883995 em is 0.003949122841783135 en is 0.005525941066065004 eo is 0.0001910865891185388 ep is 0.0014550889897322805 eq is 0.0061954518398043273325 es is 0.0037651133537430607 et is 0.0078911684082487806 eu is 0.00011182104103973751 ef is 1.132364972554304e-05 ex is 0.0005675979424928448 eq is 0.00029158398043273325 es is 0.001381485266516251 esh is 0.0011606740968681615 eш is 0.0007600999878270765 ey is 0.0 ey is 0.0 ea is 1.41545621569288e-06 eo is 0.000120313778338948 el is 0.00022364208207947502 e is 0.017674801765356993  
117 жa is 0.0013984070411045655 ж6 is 8.49273729415728e-06 жв is 2.83091243138576e-06 жr is 1.22318432353932e-05 жd is 0.0007374526883759904 жe is 0.003088525462641864 жж is 5.66182486277152e-06 жз is 0.0 жи is 0.0014239489529870373 жй is 0.0 жк is 0.00015286927129483103 жл is 2.12318432353932e-05 жм is 2.406275566677896e-05 жн is 0.0008761673975138927 жо is 6.511098592187248e-05 жп is 1.41545621569288e-06 жр is 1.981638701970032e-05 жс is 2.83091243138576e-06 жт is 0.0 жу is 0.0003821731782370776 жф is

таб. 6

H = 36.3867

/6 Bigram cross, with spaces  
77 aa is 2.3355027558932518e-05 a6 is 0.0010177130190831807 ae is 0.0026001930682278203 ar is 0.0005973225230223953 ad is 0.0017962139377142646 ae is 0.0033390612128195037 ak is 0.0013163742805943784 aa is 0.003162129185857894 ai is 0.00018684022047146015 ай is 0.0006093539008557848 ак is 0.005241434366710734 an is 0.007540842989103818 am is 0.0033461384938979683 am is 0.0027141372935910973 ao is 6.157234538264028e-05 an is 0.0008245032456411026 ap is 0.0019243127252344704 ac is 0.003619321543526694 at is 0.004509643503197516 ay is 0.00013234515616728428 aф is 0.00011465195347112327 ax is 0.0011153794979659895 au is 0.00010899012860835176 av is 0.0013234515616728428 aw is 0.0009065997061512896 ay is 0.00034254040419767697 az is 0.0 аь is 0.0 аа is 2.12318432353932e-06 ae is 0.0020333028538428223 ая is 0.0021564475446081027 a is 0.013373938053974176  
78 6a is 0.0013008042622217567 66 is 1.344683404908236e-05 6b is 2.689366809816472e-05 6r is 1.627774648046812e-05 6d is 1.06159216179696e-05 6e is 0.0018266462463516616 6ж is 1.203137783338948e-05 6a is 1.344683404908236e-05 6b is 0.0008747519412981999 6й is 0.0 6к is 0.0001358837967065165 6л is 0.00069215808994738183 6м is 4.104823025509352e-05 6н is 0.00026610576855026145 6o is 0.0018549553706655193 6п is 0.0 6р is 0.0010191284752988736 6с is 0.00019179431722638523 6т is 8.49273729415728e-06 6у is 0.00111042540121110643 6ф is 0.0 6х is 2.12318432353932e-05 6ц is 6.36955297061796e-06 6ч is 5.66182486277152e-06 6ш is 6.36955297061796e-06 6щ is 0.0003099849112367407 6ы is 0.002819588781660217 6ь is 0.00021798025721670353 6а is 0.0 6б is 4.95409675492508e-06 6б is 0.0006220930067970207 6 is 0.00021373388856962488  
79 va is 0.005771522719487718 v6 is 9.20046540200372e-06 vв is 4.034050214724708e-05 vr is 1.4154562156928799e-05 vd is 0.00023850437234425027 ve is 0.004019187924459933 vx is 7.0772810784643995e-06 va is 0.00045082280469818225 vi is 0.0024989879488057794 vй is 0.0 vk is 0.00022151889775593573 vl is 0.0007183440294641366 vm is 0.00010120511942204092 vn is 0.0.0009158001715532933 vo is 0.0058698969264783735 vp is 0.0001861324932636137 wr is 0.0006949890019052041 ws is 0.002571883943913963 wt is 0.0003099849112367407 wу is 0.000568305760606913 wf is 7.0772810784644e-07 wx is 3.963277403940064e-05 wц is 2.972458052955040e-05 wч is 7.360372321602975e-05 wш is 0.0007381604164838369 wш is 0.00072810784644e-07 wy is 0.002396367373168046 wь is 0.00010686694428481244 wа is 0.0 wб is 2.12318432353932e-06 wб is 0.0003290935701485946 w is 0.005356086320181858  
80 ra is 0.0012045523295546408 r6 is 7.0772810784644e-07 ri is 1.7693202696160999e-05 rr is 1.41545621569288e-06 rd is 0.0011543045438975436 re is 0.0001344683404908236 rg is 0.0 rз is 4.95409675492508e-06 ri is 0.000831580526719567 rй is 0.0 rk is 8.209646051018704e-05 rl is 0.0014097943908301085 rm is 1.203137783338948e-05 rn is 0.00025761303125610417 ro is 0.007516072505329193 ri is 1.41545621569288e-06 rp is 0.00084927329415728 rc is 1.4154562156928799e-05 rr is 4.034050214724708e-05 ry is 0.0005909529700517774 rf is 0.0 rх is 0.0 rц is 0.0 rч is 4.95409675492508e-05 rw is 3.5386405392321998e-06 rц is 0.0 rи is 0.0 rь is 0.0 rа is 0.0 rб is 0.0 rв is 0.0 rг is 0.0 rд is 0.0 rе is 0.000571136583032077  
81 da is 0.0038726882061357196 d6 is 6.864962646110468e-05 dа is 0.0009398629272200723 dr is 1.273910594123592e-05 dd is 2.547821188247184e-05 de is 0.003962569675832217 dj is 7.218826700033687e-05 dз is 9.90819350985016e-06 di is 0.0022350053645790575 di is 0.0 dk is 0.0002356734599128645 dl is 0.0006079384446400919 dm is 5.520279241202232e-05 dn is 0.0014862290264775239 do is 0.0039639851320479105 dp is 0.00014154562156928798 dr is 0.0010700848990638173 ds is 0.0002491202939619469 dt is 0.00022788845072655367 du is 0.0016447601226351265 df is 0.0 dk is 5.6618248627715196e-05 di is 0.00011040558482404464 dч is 2.406275566677896e-05 dш is 8.13887324023406e-05 di is 7.0772810784644e-07 dy is 0.000725423110542601 dz is 0.0004678082792864968 dz is 7.0772810784644e-07 dy is 1.132364972554304e-05 dy is 0.0004232214084921711 dz is 0.0012427705573783486  
82 ea is 5.095642376494368e-05 e6 is 0.0013149588243786855 ev is 0.0013453911330160823 er is 0.003366662609025515 ed is 0.0025669298471590377 ee is 0.001338313851937618 ej is 0.0007183440294641366 ez is 0.00120879960802017194 ei is 7.43114513238762e-05 ey is 0.001615035542105576 ek is 0.0011684591060544724 el is 0.0045683849361487705 em is 0.003964692860155757 en is 0.005477107826623599 eo is 0.00017622429885376357 ep is 0.001462166270810745 eq is 0.00599304617243654 es is 0.003726896215919353 et is 0.007957694844625371 eu is 0.00011040558482404464 ef is 1.557001837262168e-05 ex is 0.0005654747581693055 eq is 0.00029016852421704037 еч is 0.0014260721373015766 еш is 0.0011557200001132365 eu is 0.00076717726809545049 eu is 0.0 ey is 0.0 ea is 2.12318432353932e-06 eo is 0.00011606740968681615 es is 0.00022364208207947502 e is 0.01759966198905568  
83 жa is 0.00138313851937618 ж6 is 7.0772810784643995e-06 жв is 4.24636864707864e-06 жr is 2.264729945108608e-05 жd is 0.0007735468218761589 же is 0.0030276600453670703 жж is 1.06159216179696e-05 жз is 0.0 жи is 0.001431733962173348 жй is 0.0 жк is 0.00015357699940267747 жл is 2.264729945108608e-05 жм is 2.3355027558932518e-05 жн is

таб. 4

H = 36.406



За допомогою CoolPinkProgram було оцінено значення  $H^{10}$ ,  $H^{20}$ ,  $H^{30}$ .

Лабораторная работа №1

Произвольная часть текста:  
ставить\_на\_первое\_место\_самого\_себя\_эгоизм\_никогда\_и\_нигде\_не\_считался\_похв

Использованные буквы:

Порядок n-граммы:  
5 символов  
15 символов  
20 символов  
25 символов  
30 символов  
35 символов  
40 символов  
45 символов  
50 символов

Введенный символ: а

Символ по счету: 1

Номер эксперимента: 50

Неравенство для энтропии:  
 $1,94072451102478 < H < 2,74791993994523$

Двоичная таблица угаданных символов:

01000000000000000000000000000000
00000000000000000000000000000000
00000100000000000000000000000000
10000000000000000000000000000000
10000000000000000000000000000000

Поле ввода символов:  
а

Продолжить Другой

Вероятности:

q[1] = 0,46
q[2] = 0,16
q[3] = 0,04
q[4] = 0,08
q[5] = 0,06
q[6] = 0,02
q[7] = 0
q[8] = 0,04
q[9] = 0
q[10] = 0,02
q[11] = 0
q[12] = 0,02
q[13] = 0
q[14] = 0
q[15] = 0
q[16] = 0
q[17] = 0
q[18] = 0,02
q[19] = 0,02
q[20] = 0
q[21] = 0,02
q[22] = 0
q[23] = 0
q[24] = 0
q[25] = 0
q[26] = 0,02
q[27] = 0
q[28] = 0
q[29] = 0
q[30] = 0,02
q[31] = 0
q[32] = 0

Строка состояния:  
Вы угадали. Для продолжения опыта нажмите "Продолжить", или "Другой" для выбора другого порядка

$$H^{10} = \frac{1,94 + 2,75}{2} = 2,345$$

Лабораторная работа №1

Произвольная часть текста:  
ему\_закону\_человеческой\_природы\_или\_нарушать\_его\_ту\_же\_идею\_можно\_выразить\_

Использованные буквы:

Порядок n-граммы:  
5 символов  
10 символов  
15 символов  
20 символов  
25 символов  
30 символов  
35 символов  
40 символов  
45 символов  
50 символов

Введенный символ: с

Символ по счету: 1

Номер эксперимента: 51

Неравенство для энтропии:  
 $0,708623630463532 < H < 1,1130408664833$

Двоичная таблица угаданных символов:

10000000000000000000000000000000
10000000000000000000000000000000
10000000000000000000000000000000
10000000000000000000000000000000
10000000000000000000000000000000

Поле ввода символов:  
с

Продолжить Другой

Вероятности:

q[1] = 0,7843137
q[2] = 0,1372549
q[3] = 0
q[4] = 0
q[5] = 0
q[6] = 0
q[7] = 0
q[8] = 0
q[9] = 0
q[10] = 0,019607
q[11] = 0
q[12] = 0
q[13] = 0
q[14] = 0
q[15] = 0
q[16] = 0,019607
q[17] = 0
q[18] = 0
q[19] = 0
q[20] = 0,019607
q[21] = 0
q[22] = 0
q[23] = 0
q[24] = 0
q[25] = 0
q[26] = 0
q[27] = 0
q[28] = 0
q[29] = 0
q[30] = 0,019607
q[31] = 0
q[32] = 0

Строка состояния:  
Вы угадали. Для продолжения опыта нажмите "Продолжить", или "Другой" для выбора другого порядка

$$H^{20} = \frac{0,71 + 1,11}{2} = 0,91$$

[illegible]

$$H^{30} = \frac{1,36 + 2,07}{2} = 1,715$$

$N_0$  для заданого алфавіту –  $\log_2 32=5$ , тоді:

$$\begin{aligned} 1) \quad R &= 1 - \frac{2,345}{5} = 0,531 \\ 2) \quad R &= 1 - \frac{0,91}{5} = 0,818 \\ 3) \quad R &= 1 - \frac{1,715}{5} = 0,65 \end{aligned}$$

Середнє значення  $R$  надлишковості російської мови – 0,666, але кількість проведених експериментів ніяк не прямує до нескінченності, тому можуть виникати значні похибки.

**Висновки:** після виконання цієї лабораторної роботи в нас з'явилося більш чітке уявлення про поняття ентропії не лише у вигляді формули, а на конкретному прикладі мови. Підтвердили, що не має істотної різниці у розподілі частот при підрахунку їх для біграм з перетином і без, що свідчить про коректність програми.

І з першої, і з другої частини роботи побачили, як часто зустрічається пробіл. Друга частина показала, що надлишковість російської мови – приблизно 66%, що свідчить про повторюваність значної кількості інформації, але є цілком природнім для усіх мов.

Також було отримано навички роботи з мовою Python та системою Git.